Walder Intellectual Property Law, P.C.
17330 Preston Rd., Suite 100B
Dallas, TX 75252
Main No. (972) 380-9475
Facsimile (972) 733-1575

Facsimile Cover Sheet

To: Examiner Techane Gergiso Art Unit 2437 U.S. Patent and Trademark Office	Facsimile No. 571-273-3784 Telephone No. 571-272-3784
From: Stephen J. Walder, Jr. Sent by: Rebecca Clayton, Admin. Asst.	No. of Pages Including Cover Sheet: 9

Message:

Examiner Gergiso,

Following is an agenda including proposed claim amendments for discussion during a telephone interview for the application referenced below. Would you be available for a telephone interview on Friday, 02/05/10, at 2:00 p.m. (EST)? Please call me at the number above to let me know if you would be available on the proposed date and time. If not, I will be happy to check Steve's calendar for an alternate date.

Thank you.

Serial No. 10/803,590; Attorney Docket No. AUS920031041US1

Date: Thursday, January 28, 2010

Please contact us at (972) 380-9475 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	

AGENDA FOR TELEPHONE INTERVIEW

Serial No. 10/803,590 Docket No. AUS920031041US1

I. **Overview of Claimed Invention**

II. **Overview of Cited Art**

III. **Overview of Claim Amendments**

IV. **Discussion of Art Rejections**

A. **Claim Objections**

The Office Action objects to claims 1, 28, and 33 for various informalities. Claims 1, 28, and 33 are amended where appropriate to eliminate these formalities.

B. **Rejection under 35 U.S.C. § 112, Second Paragraph**

1. With regard to claim 1, the Office Action alleges that because the claim recites at least three devices, i.e. a source device, an intermediate device, and a target device to form the path that somehow this invalidates the recitation of "a next device in the transmission path" and renders the claim indefinite. Applicants respectfully disagree.

2. Simply reciting at least 3 devices does not invalidate a recitation of a "next device." If one is transmitting from a first device to a second device, then the second device is the "next device" along the path. Thus, for example, if the transmission is going from the source device to the intermediate device, then the intermediate device is the "next device" along the path. Similarly, if the intermediate device is transmitting to a target device, then the target device is the "next device" along the path. The phrase "next device" along the path is specifically used in the claims because there may actually be more than one intermediate device and thus, it is possible that the "next device" is not a single intermediate device or the target device, but can be a second, third, fourth, etc., intermediate device. All that is required is that a determination is made as to whether a "next device" in the transmission path, be that any one of the one or more intermediate devices or the target device, to which the object is to be transmitted, provides a level of security indicated by at least a portion of the security information in the header of the object. Thus, the recitation of the phrase "a next device in the transmission path" does not render the claim indefinite.

3. Regarding claim 3, it is Applicants' understanding that the Office Action alleges that the claim does not recite a plurality of alternatives from which "at least one of" the alternatives is performed. By this Response, claim 3 is amended to more clearly recite the alternatives by replacing the term "and" with "or." Accordingly, Applicants respectfully submit that claim 3 clearly recites the alternatives of either "transmitting information representative of the level of security that is desired to the next device in the transmission path which prompts the next device in the transmission path to execute at

least one module that allows the next device in the transmission path to provide the level of security" ***or*** "comparing the next device in the transmission path to a list of trusted devices in the header portion of the object."

C. Rejection under 35 U.S.C. § 103(a)

1. Suzuki is directed to a wireless adhoc communication system in which frame transmission source authentication is performed among terminals involved in delivery of the frames. Specifically, a first terminal generates a keyed hash value by using an authentication header key determined with respect to a second terminal and gives it to an authentication header of a frame. The second terminal generates a keyed hashed value by using the authentication header key determined with respect to the first terminal and compares it with the authentication header given to the frame. If the keyed hashed value generated at the second terminal matches the authentication header ***it is confirmed that the frame has been transmitted from the first authenticated valid terminal.*** The first terminal encrypts a payload part by using a unicast encryption key determined with respect to a third terminal. This encrypted payload part can be decrypted only by the third terminal having the unicast encryption key (see Abstract of Suzuki).

2. Thus, essentially Suzuki is directed to validating that a frame is being sent from an authenticated valid terminal. Suzuki is not concerned with determining whether a next device along a transmission path provides a level of security indicated by at least a portion of the security information in the header of an object being transmitted. To the contrary, Suzuki is specifically looking backward to the source to determine if the source was valid. At no time in the operation of the wireless adhoc communication system of Suzuki is there any determination as to whether the next target of the transmission provides a required level of security as specified in a header of the frame.

3. Moreover, nowhere in Suzuki is there any teaching or technical rationale provided for transmitting an object along the transmission path to the next device in response to determining that the next device provides a level of security required by the portion of the security information in the header of the object. To the contrary, in Suzuki, the frame is transmitted only when it is determined that the ***source*** of the frame, i.e. the terminal that is attempting to transmit, is an authenticated valid terminal. Suzuki is not concerned with whether the next device to which the frame is being transmitted provides a required level of security as specified in a header of the frame.

4. The Office Action admits that Suzuki does not teach security information that is associated with a transaction object or providing a level of security indicated by at least a portion of the security information (see Office Action, page 5). However, the Office Action alleges that these features are taught by Lee. Applicants respectfully disagree.

5. Lee is directed to a mechanism for dynamically constructing a protocol to facilitate communication between nodes and across multiple nodes. Policies associated with the nodes are used to specify protocol properties of the nodes. A policy expression

in a policy related to a node can be selected by another node to construct a protocol between the two nodes. A policy expression selection process can be applied to multiple nodes in a communication path to construct a protocol across the multiple nodes (see paragraph [0007]). A computer can retrieve an intermediate node policy characterizing communication properties supported by the intermediate node and may request destination node policies characterizing communication properties supported by a destination node (paragraphs [0009]-[0010]).

6. With Lee, the protocol must be established first before any actual message communications are performed between a source and a destination. Lee provides a mechanism for establishing such a protocol dynamically based on the policies of the nodes between the source and destination. Essentially, the mechanism of Lee creates a protocol that is supported by all of the nodes along a communication path prior to performing any communication. This essentially means that the protocol that is created has a minimum number of protocol properties according to the lowest common denominator amongst the nodes.

7. Lee does not provide any teaching, or technical rationale, to implement the features of providing security information in a header of an object of a transaction, at least a portion of the security information identifying a required level of security required for each device along a transmission pathway, or using the portion of the security information at each device along the transmission pathway to determine if a next device along the pathway provides the required level of security and transmitting the object to the next device if the next device provides the required level of security. To the contrary, Lee is concerned with connection level protocol establishment, rather than providing a transaction level security mechanism, as is recited in claim 1. Lee is not concerned with performing security level checks on each individual device of a transmission path, whether the individual device provides a level of security required by header information an object of a transaction prior to the object being transmitted to the device and transmitting the object to that device in response to a determination that the device supports the required level of security.

PROPOSED CLAIM AMENDMENTS

1. (Currently amended) A method, comprising:

determining security information associated with [[a]] an object of a transaction, wherein the security information is inserted in a header of the object and the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device;

determining, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, whether a next device in the transmission path to which the object is to be transmitted provides a level of security indicated by at least a portion of the security information in the header of the object; and

transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, the object to the next device in the transmission path in response to determining that the next device provides the level of security required by the at least a portion of the security information.

2. (Previously presented) The method of claim 1, wherein the object is a business object, and wherein determining if the next device in the transmission path provides the level of security comprises:

transmitting to the next device in the transmission path information representative of the level of security that is desired; and

receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security.

3. (Currently amended) The method of claim 1, wherein determining the security information comprises accessing the header portion of the object;

wherein determining if the next device in the transmission path provides a level of security indicated comprises performing at least one of:

transmitting information representative of the level of security that is desired to the next device in the transmission path which prompts the next device in the transmission path to

execute at least one module that allows the next device in the transmission path to provide the level of security; [[and]] or

comparing the next device in the transmission path to a list of trusted devices in the header portion of the object;

wherein the transmitting the object to the next device in the transmission path comprises transmitting the object to an object handler module in the next device in the transmission path;

wherein the object handler module is a business integration adapter supporting connectivity options, the connectivity options comprising at least one of packaged applications, custom applications, legacy applications, databases, trading partners' systems, and public information stores on the internet;

wherein the object handler module supports at least one of event-driven real-time synchronous connections, asynchronous loosely coupled connections with trading partners, synchronous on-demand connections to customers and synchronous tightly coupled connections to trusted trading partners; and

wherein the object handler module includes at least one of a module for accessing the security information associated with a given object and a module for requesting the adjacent intermediate device in the transmission path to provide information about its security capabilities.

4. (Previously presented) The method of claim 1, wherein determining the security information comprises determining security information relating to at least one of connection information, class information, trusted entities information, and logging capability information.

5. (Original) The method of claim 3, wherein accessing the header portion of the object comprises accessing at least one header of a Simple Object Access Protocol message.

6. (Previously presented) The method of claim 1, further comprising determining an alternative device along a different transmission path that provides the level of security required by the at least a portion of the security information in response to determining that the next

device in the transmission path does not provide the level of security required by the at least a portion of the security information.

7. (Previously presented) The method of claim 1, further comprising sending a message to the next device in the transmission path instructing the next device to execute at least one module that allows the next device to provide the level of security required by the at least a portion of the security information.

8. (Previously presented) The method of claim 1, wherein determining the security information comprises determining the security information in response to receiving the object from at least one of a previous device or a source device in the transmission path.

9-27. (Cancelled)

28. (Currently amended) A method, comprising:

receiving, at a first device along a transmission path from a source device to a target device, a request from a second device along the transmission path desiring to transmit an object to a third device, wherein the request includes at least a portion of security information associated with the object, the portion of security information being provided in a header of the object;

determining if the first device ~~is adapted to provide~~ provides a level of security identified by the at least a portion of security information in the header of the object; and

transmitting an indication to the second device, based on determining if the first device provides the level of security identified by the at least a portion of security information; and

receiving, in the first device, the object from the second device only in response to the first device transmitting an indication that the first device provides the level of security identified by the at least a portion of security information.

29. (Previously presented) The method of claim 28, further comprising configuring the first device with at least one module that provides the level of security.

30. (Cancelled)

31. (Previously presented) The method of claim 1, wherein at least one intermediate device includes at least a first intermediate device and a second intermediate device;

wherein determining if a next device in the transmission path provides a level of security required by the at least a portion of security information includes performing the determining at the source device, wherein the next device is the first intermediate device;

wherein transmitting the object to the next device comprises transmitting the object to the first intermediate device, and wherein in response to determining that the next device provides the level of security, and in response to determining that the first intermediate device provides the level of security:

determining, at the first device, if a second device of the plurality of intermediate devices that is adjacent the first device provides the level of security indicated by the at least a portion of the security information;

transmitting the object to the second device of the plurality of intermediate devices in response to determining that the second device provides the level of security; and

transmitting the object to the target device from the second device.

32. (Previously presented) The method of claim 31, further comprising determining an alternative intermediate device along a different transmission path that provides the level of security represented in response to determining that at least one of the first intermediate device and the second intermediate device in the transmission path does not provide the level of security.

33. (Currently amended) The method of claim 1, wherein the at least one intermediate device includes a plurality of intermediate devices;

wherein determining if a next device in the transmission path provides a level of security comprises determining, at a previous device in the transmission path, a security level for each intermediate device of the plurality of intermediate devices; and

wherein transmitting the object to the next device in the transmission path, in response to determining that the next device ~~is adapted to provide~~ provides the level of security, comprises transmitting the object to each of the plurality of intermediate devices in the transmission path in response to determining that each of the plurality of intermediate devices provides the level of security[[;]]

~~further comprising:~~

~~transmitting the object to the target device~~.

34. (Previously presented) The method of claim 1, wherein the object is one of a plurality of objects of the transaction, and wherein at least two of the objects in the plurality of objects have different security information in their respective headers identifying different levels of security required to be provided by devices along corresponding transmission paths to receive the at least two objects.